ABSTRACT OF THE DISCLOSURE

A security infrastructure is described that enables a highly secure, dynamic, robust, and extensible security infrastructure. The security infrastructure uses integrated circuits (TEIs) that generate a unique set of output values in response to receiving a given set of "input seed values". The particular output values generated by a TEI in response to input seed values cannot, for all practical purposes, be predicted. "Trusted Objects" (TOs) are data structures that are encrypted using keys generated from the unique set of output values generated by one or more TEIs in response to input seed values applied to those TEIs. The keys are formed using a key generation process that computes keys from the TEI output values. Thus, the keys may be regenerated by later applying the same input seed values to the TEIs, and applying the resultant output values to the key generation process to reproduce the original keys.